UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

OMAR ABDULAZIZ,

Plaintiff,

v.

TWITTER, INC., and MCKINSEY & CO.,

Defendants.

Case No. 19-cv-06694-LB

ORDER GRANTING THE DEFENDANTS' MOTIONS TO DISMISS

Re: ECF Nos. 41 & 43

INTRODUCTION

The plaintiff Omar Abdulaziz is a political dissident who moved to Canada in 2009 and was granted political asylum there (in 2014) based on the Kingdom of Saudi Arabia's persecution of him.[1] In this lawsuit, he alleges that in 2014, Saudi authorities recruited two employees of the social-media company Twitter to access his confidential Twitter data and thereafter used malware in 2018 to hack his phone (and obtain texts, emails, and other information) and then targeted his family.[2] Based on this conduct, he sued Twitter for (1) violating the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, (2) violating California's Unfair Competition Law ("UCL"),

[1] First Am. Comp. ("FAC") – ECF No. 38 at 3 (¶ 9), 5 (¶ 15). Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] *Id.* at 11–14 (¶¶ 47–72), 19–20 (¶¶ 101–05).

Cal. Bus. & Prof. Code § 17200, *et seq.*, (3) common-law invasion of privacy, (5) intentional and negligent misrepresentation and concealment (for misrepresenting that a bug in its system had been fixed), and (6) negligent hiring, supervision, or retention of employees.[3] He also sued the consulting firm McKinsey & Co. for intentional infliction of emotional distress, a claim that he predicates on McKinsey's allegedly identifying him to Saudi authorities — based on internal Twitter data — as shaping opinion in Saudi Arabia.[4]

Twitter moved to dismiss the claims against it for lack of Article III standing and for failure to state a claim.[5] McKinsey moved to dismiss for lack of personal jurisdiction and for failure to state a claim.[6] The court grants the motions to dismiss.

For the claims against Twitter, there is no Article III standing. Even if there were, the plaintiff does not plead plausibly that Twitter ratified its rogue employees' acts on behalf of Saudi agents or otherwise has *respondeat superior* liability, which disposes of all claims except the hiring claims. The statute of limitations bars those claims (and all claims except the UCL claim). Other grounds support dismissal too, such as failure to plead the misrepresentation and concealment claims with particularity under Fed. R. Civ. P. 9(b).

There is no personal jurisdiction for the claim against McKinsey.

STATEMENT

1. The Plaintiff's Political Activism

In 2009, the plaintiff moved from Saudi Arabia to Montreal, Canada to attend a Canadian university.[7] As a student, the plaintiff discussed Saudi Arabian politics on Twitter and other social-media platforms, criticizing the governing regime and the royal family.[8] In retaliation for

[3] *Id.* at 22–30 (¶¶ 114–78).
[4] *Id.* at 5–6 (¶ 18) (citing McKinsey Report, Ex. A to FAC – ECF No. 38 at 41).
[5] Twitter Mot. – ECF No. 41.
[6] McKinsey Mot. – ECF No. 43.
[7] FAC – ECF No. 38 at 3 (¶ 9).
[8] *Id.*

his activities, the Saudi government harassed him, and the plaintiff sought political asylum in Canada in December 2013 and received it on February 21, 2014.[9] In response to the harassment, the plaintiff increased his criticism of Saudi Arabia and became especially popular among Saudi youth.[10] The plaintiff also contributes to and co-manages a number of websites, Twitter accounts, and YouTube channels.[11] In 2015, he had fewer than 200,000 Twitter followers and even fewer subscribers to his YouTube channel.[12] Today, the plaintiff has over 400,000 followers on Twitter and over 163,000 subscribers to his YouTube channel.[13]

2. Saudi Arabia Obtained Information About the Plaintiff

In addition to its access to publicly available information about the plaintiff, Saudi Arabia obtained information about the plaintiff through three means: (1) his private Twitter information accessed unlawfully by Twitter employees; (2) planting malware on his phone and then hacking the phone; and (3) a McKinsey report.[14]

2.1 Twitter Employees Gain Access to the Plaintiff's Twitter Information

Twitter is incorporated in Delaware and has its headquarters in San Francisco.[15]

Saudi Arabia allegedly recruited two Twitter employees — Ali Alzabarah (a Saudi citizen and a U.S. resident since 2005 and a site-reliability engineer for Twitter from August 2013 to December 2015) and Ahmad Abouammo (an American citizen and a Media Partnerships Manager for Twitter for the Middle East and North Africa region from November 2013 to May 2015) — to access certain Twitter accounts without Twitter's authorization.[16] Abouammo began the

---

[9] *Id.* at 5 (¶ 15).
[10] *Id.* (¶ 16).
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.* at 11–14 (¶¶ 47–72), 19–20 (¶¶ 101–05), 16–17 (¶ 87), 5–6 (¶ 18).
[15] *Id.* at 2 (¶ 3).
[16] *Id.* at 6–7 (¶¶ 22–23), 9–10 (¶¶ 34–43), 12–13 (¶¶ 63–64).

unauthorized access in December 2014, and Alzabarah began in May 2015.[17] The plaintiff alleges that Alzabarah accessed his confidential information, including his passwords, IP addresses, and direct messages in June and July 2015.[18] Federal prosecutors investigated the unauthorized access and ultimately charged both criminally on November 5, 2019 with acting as agents of a foreign government in violation of 18 U.S.C. § 951.[19]

When Twitter learned about the unauthorized access, on December 2, 2015, it placed Alzabarah on leave, seized his company laptop, and escorted him from the building.[20] Alzabarah then decamped to Saudi Arabia with his family.[21] (Abouammo left his job at Twitter earlier that year.[22]) Shortly after Alzabarah fled, Saudi authorities interviewed the plaintiff's father and brother in Saudi Arabia, cancelled the brother's financial assistance, and imprisoned many of the plaintiff's friends in Saudi Arabia.[23]

On December 11, 2015, by email and through an in-app message, Twitter notified the owners of the accounts that had been compromised, including the plaintiff, that their Twitter accounts may have been targeted by state-sponsored actors to obtain IP addresses, emails, and phone data.[24] The plaintiff alleges that he did not receive the notices and instead learned about the unauthorized access when he read about it in the New York Times on October 20, 2018.[25] If he had known that his account had been compromised, then he would have been more careful about clicking on

---

[17] *Id.* at 12 (¶ 56), 13 (¶ 65).

[18] *Id.* at 13–14 (¶¶ 70–72).

[19] *United States v. Abouammo et al.*, Case No. 3:19-MJ-71824-MAG (N.D. Cal.); *id.*, No. 19-cr-00621-EMC (N.D. Cal.) (the indicted case).

[20] *Abouammo*, Compl. No. 1 at 23–24 (¶ 85), Compl. – ECF No. 1 at 9 (¶ 47); FAC – ECF No. 38 at 15 (¶ 79).

[21] *Abouammo*, Compl. No. 1 at 25 (¶ 88), Compl. – ECF No. 1 at 9 (¶ 47); FAC – ECF No. 38 at 15 (¶ 80).

[22] *Abouammo*, Compl. No. 1 at 5 (¶ 17); FAC – ECF No. 38 at 13 (¶ 67).

[23] FAC – ECF No. 38 at 18 (¶ 93).

[24] Notifications, Exs. 1 & 2 to Twitter Employee Decl. – ECF Nos. 41-6 & 41-7. The court considers the notices under the incorporation-by-reference doctrine (given the complaint's reference to them at paragraph 88). *Knievel v. ESPN*, 393 F.3d 1068, 1076–77 (9th Cir. 2005).

[25] FAC – ECF No. 38 at 18 (¶ 96).

hyperlinks in text messages and would not have clinked on the link that put malware on his phone and allowed Saudi operatives to hack his phone.[26]

In support of his contention that Twitter is responsible for the unauthorized act of its employees (even though those actions violated company policy), the plaintiff alleges the conduct was a "red flag" that should have alerted Twitter to the illegal activity.[27] The plaintiff also alleged that the danger "was inherent in Twitter's manner of operation:"

> First, Twitter furnished Alzabarah and Abouammo with the access, hardware and software tools that enabled them to raid Plaintiff's private information. This would not have been possible were they not employed by Twitter. Second, Twitter implemented and benefited from policies that allowed and encouraged its technical and professional staff to work offsite, from multiple locations. Although Twitter benefitted from the greater productivity this allowed, it even further reduced Twitter's ability to monitor sensitive employees' conduct. Finally, Twitter implemented and benefitted from policies allowing its professional and technical staff flexibility as to when and where they performed their work, further complicating any monitoring Twitter should have been doing. With hundreds of millions of active users and a great many employees who had access to their data, the risk that confidential data would be exposed was broadly incident to Twitter's mode of operation.[28]

Despite the known risks, Twitter "failed to institute adequate safeguards to protect this data or even alert Twitter senior management that private account data was being raided."[29] Also, Twitter did not institute appropriate safeguards or notify the plaintiff or other victims that it wanted to maintain its relationship with Saudi Arabia (shown in part by Saudi holdings in Twitter and a meeting that Twitter CEO Jack Dorsey had with Crown Prince Mohammed Bin Salman six months after Alzabarah fled to Saudi Arabia).[30]

In February 2016, Twitter sent a notice (unrelated to the Saudi access to the Twitter accounts) that Twitter had "recently learned about — and immediately fixed — a bug that affected our

---

[26] *Id.* (¶ 90).

[27] *Id.* at 6–7 (¶¶ 22–23), 10–11 (¶¶ 43–46), 12–15 (¶¶ 63–79).

[28] *Id.* at 14 (¶ 74).

[29] *Id.* (¶ 75).

[30] *Id.* at 15–16 (¶¶ 82–84).

password recovery systems for about 24 hours last week. The bug had the potential to expose the email address and phone number associated with a small number of accounts."[31]

2.2 Saudi Operatives Hack the Plaintiff's Phone

In May 2018, two Saudi agents contacted the plaintiff, asked to meet with him, and met with him in several meetings.[32] The agents said that they worked for Crown Prince Bin Salman and Saud Al-Qahtani (who was "entangled with the murder of" Jamal Khashoggi) and demanded that the plaintiff stop his political activities and return to Saudi Arabia.[33] The plaintiff refused.[34] At one meeting, just a few months before Saudi assassins murdered Mr. Khashoggi, the agents "arranged for Plaintiff's younger brother to be present as a message that they can reach and harm Plaintiff's family."[35]

On June 23, 2018, Saudi agents planted Pegasus malware on the plaintiff's phone in a phishing direct message masquerading as a message from the shipping company DHL to manage a delivery.[36] As a result, the agents exfiltrated the plaintiff's SMS chats, emails, photographs, location data, and other information and were able to spy on the plaintiff "real time" through control of the phone's camera and microphone and receipt of information that the plaintiff typed into the phone or received from others.[37]

In late July and early August 2018, Saudi agents raided the plaintiff's family home in Jeddah, Saudi Arabia.[38] Saudi police arrested two of his brothers.[39] They are still in prison, without charge, and are being tortured to pressure the plaintiff to stop his activism.[40] Saudi agents have also

---

[31] *Id.* at 17 (¶ 89) (citing Twitter Notification, Ex. B to FAC, ECF No. 38 at 43–46).
[32] *Id.* at 18–19 (¶¶ 97–98).
[33] *Id.*
[34] *Id.*
[35] *Id.* (¶ 99).
[36] *Id.* at 19–20 (¶¶ 101–02).
[37] *Id.* at 20 (¶¶ 104–05).
[38] *Id.* (¶ 107).
[39] *Id.*
[40] *Id.*

imprisoned, tortured, and humiliated dozens of the plaintiff's friends and associates in Saudi Arabia to pressure the plaintiff to stop his activism.[41]

In mid-August 2018, the Citizens Lab at the University of Toronto told the plaintiff about the compromise of his phone through the Pegasus malware.[42] In December 2018, in a separate lawsuit filed in Israel, the plaintiff sued N.S.O. Technologies, which manufactures the Pegasus software, on the ground that is liable for the hacking of his phone and the resulting harm that he and his family and friends suffered.[43]

2.3 The McKinsey Report

McKinsey is incorporated in New York and has its principal place of business there.[44]

In December 2016 or 2017, in a PowerPoint presentation, McKinsey "singled out Plaintiff to agents of Prince Mohammed bin Salman by identifying Plaintiff as one of the top three voices shaping public discussion about controversial austerity measures."[45] (The two others were Khaled Al-Alkami, who was imprisoned after he was identified, and "Ahmad," who "disappeared."[46]) The plaintiff alleges that McKinsey based its report on its analysis of Twitter data.[47] He alleges on information and belief that McKinsey bought the data from Twitter.[48] (Twitter and McKinsey assert that they had no agreement whereby McKinsey bought Twitter data.[49] Both contend that the PowerPoint is obviously based on publicly available Twitter feeds.[50])

---

[41] *Id.* at 21 (¶ 109).

[42] *Id.* (¶ 110).

[43] Statement of Claim, Ex. A to Olm Decl. – ECF No. 41-2 at 1. The court takes judicial notice of court records of the lawsuit. *Lee v. City of Los Angeles*, 250 F.3d 668, 689–90 (9th Cir. 2001); *United States ex rel. Robinson Rancheria Citizens Council v. Borneo, Inc.*, 971 F.2d 244, 248 (9th Cir. 1992).

[44] FAC – ECF No. 38 at 2 (¶ 4); Duffy Decl. – ECF No. 43-1 at 2 (¶ 3).

[45] FAC – ECF No. 38 at 5–6 (¶ 18).

[46] *Id.*

[47] *Id.* at 6 (¶ 19).

[48] *Id.* (¶¶ 19–20).

[49] Twitter Mot. – ECF No. 41 at 12 n.3; Brennan Decl. – ECF No. 43-2 at 2–3 (¶ 4).

[50] Twitter Mot. – ECF No. 41 at 12 n.3; McKinsey Mot. – ECF No. 43 at 15; *see id.* at 15–16 (the October 20, 2018 New York Times article was corrected and ultimately reflected that the PowerPoint was an internal McKinsey document, not a document prepared for the Saudi government) (citing *DealBook Briefing, It's Tough to Quit Saudi Arabia*, N.Y. Times (Oct. 22, 2018)).

3. Procedural History

The plaintiff filed his initial complaint on October 18, 2019 against Twitter and McKinsey.[51] After Twitter and McKinsey moved to dismiss, the parties stipulated to the plaintiff's amending his complaint, and he filed the FAC on February 11, 2020.[52] All parties have consented to the undersigned's jurisdiction.[53] The court held a hearing on August 6, 2020.

STANDARD OF REVIEW

A complaint must contain a short and plain statement of the ground for the court's jurisdiction (unless the court already has jurisdiction and the claim needs no new jurisdictional support). Fed. R. Civ. P. 8(a)(1). The plaintiff has the burden of establishing jurisdiction. *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994); *Farmers Ins. Exch. v. Portage La Prairie Mut. Ins. Co.*, 907 F.2d 911, 912 (9th Cir. 1990).

A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief" to give the defendant "fair notice" of what the claims are and the grounds upon which they rest. Fed. R. Civ. P. 8(a)(2); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint does not need detailed factual allegations, but "a plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual allegations must be enough to raise a claim for relief above the speculative level[.]" *Twombly*, 550 U.S. at 555 (cleaned up).

To survive a motion to dismiss, a complaint must contain sufficient factual allegations, which when accepted as true, "'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "The plausibility standard is not akin to a

[51] Compl. – ECF No. 1 at 10–18 (¶¶ 50–112).

[52] Stipulated Order – ECF No. 37; FAC – ECF No. 38.

[53] Consent Forms – ECF Nos. 10, 20, and 21.

'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (citing *Twombly*, 550 U.S. at 557). "Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of 'entitlement to relief.'" *Id.* (cleaned up) (quoting *Twombly*, 550 U.S. at 557).

Fraud allegations elicit a more demanding standard. Rule 9(b) provides: "In alleging fraud . . ., a party must state with particularity the circumstances constituting fraud . . . . Malice, intent, knowledge, and other conditions of a person's mind may be alleged generally." Fed. R. Civ. P. 9(b). This means that "[a]verments of fraud must be accompanied by the 'who, what, when, where, and how' of the misconduct charged." *Vess v. Ciba–Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). Like the basic "notice pleading" demands of Rule 8, a driving concern of Rule 9(b) is that defendants be given fair notice of the charges against them. *See, e.g., In re Lui*, 646 F. App'x 571, 573 (9th Cir. 2016) ("Rule 9(b) demands that allegations of fraud be specific enough to give defendants notice of the particular misconduct . . . so that they can defend against the charge and not just deny that they have done anything wrong.") (quotation omitted); *Odom v. Microsoft Corp.*, 486 F.3d 541, 553 (9th Cir. 2007) (Rule 9(b) requires particularity "so that the defendant can prepare an adequate answer").

If a court dismisses a complaint, it should give leave to amend unless the "pleading could not possibly be cured by the allegation of other facts." *Yagman v. Garcetti*, 852 F.3d 859, 863 (9th Cir. 2017) (citations and internal quotation marks omitted).

ANALYSIS

Twitter and McKinsey filed separate motions to dismiss. The court grants both motions.

1. Twitter's Motion to Dismiss

The plaintiff claims the following: (1) Twitter violated the SCA by ratifying its employees' intentional access of his Twitter information (claim one); (2) that same conduct is an unlawful, unfair, and fraudulent and deceptive practice under California's UCL (claim two); (3) the access of his private data constitutes common-law invasion of privacy (claim three); (4) the February

2016 notice about the bug misled the plaintiff into believing that his Twitter account had not been hacked and was intentional and negligent misrepresentation and concealment (claims five, six, and seven); and (5) Twitter hired Alzabarah and Abouammo, they became unfit employees, and Twitter knew or should have known that they were unfit, thereby amounting to negligent hiring, supervision, or retention of employees (claim eight).[54]

The court grants Twitter's motion to dismiss on the following grounds: (1) lack of Article III standing (for all claims); (2) failure to plausibly plead ratification and *respondeat superior* liability (for all claims but claim eight); (3) the statutes of limitations bars all claims but claim two; and (4) other defects require dismissal.

1.1 Article III Standing

Federal-court jurisdiction extends only to "cases" and "controversies." *Raines v. Byrd*, 521 U.S. 811, 818 (1997); *see Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). To establish standing, "[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.* (citing *Lujan v Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). As to the causation prong, Article III requires "a causal connection between the injury and the conduct complained of — the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.'" *Lujan*, 504 U.S. at 560–61 (quoting *Simon*, 426 U.S. at 41–42) (ellipses in original). "[S]tanding in federal court is a question of federal law, not state law." *Hollingsworth v. Perry*, 570 U.S. 693, 715 (2013).[55]

Twitter's rogue employees accessed the plaintiff's Twitter data in June and July 2015. The alleged immediate harm ("shortly" after Alzabarah fled to Saudi Arabia in December 2015) was the questioning of the plaintiff's father and brother, the loss of his brother's financial benefits (at

[54] FAC – ECF No. 38 at 22 (¶¶ 115–117) (SCA claim), 23 (¶¶ 123–125) (UCL claim), 25 (¶¶ 131–135) (common-law invasion-of-privacy claim), 26–27 (¶¶ 147–151) (intentional-misrepresentation claim), 27–28 (¶¶ 156–160) (negligent-misrepresentation claim), 28–29 (¶¶ 164–168) (concealment claim), 30 (¶¶ 173–175) (claim for negligent hiring, supervision, or retention of employees).

[55] This disposes of the plaintiff's argument that — assuming that there is no federal-question jurisdiction (based on the SCA claim) and instead there is diversity jurisdiction for the state claims — California causation standards apply. Opp'n – ECF No. 58 at 10.

some undisclosed time), and the imprisonment of many of the plaintiff's friends in Saudi Arabia (again at an undisclosed time).[56] The hacking of the plaintiff's phone was in late July and early August 2018, resulting in the compromise of his data, the raid of his family home in Saudi Arabia, the arrest and imprisonment of his brothers, and the persecution of his friends.[57]

These facts do not plausibly establish that Twitter's alleged misconduct caused the harms. First, the plaintiff does not explain how the compromise of the Twitter data caused the harm to his family and friends that happened shortly after Alzabarah fled to Saudi Arabia. Indeed, he is a political dissident with an active social-media presence who suffered persecution before the compromise of his Twitter data (shown by Canada's granting him political asylum in February 2014). Second, the implanting of the Pegasus malware and the subsequent compromise of his data in July and August 2018 was three years after the compromise of his Twitter data. There is no temporal proximity. And the plaintiff's allegation that it is related to the Twitter breach is a conclusion, not a fact allegation. In sum, the plaintiff does not plausibly plead causation and thus did not establish Article III standing.

1.2 Twitter Notices in December 2015 and February 2016

Even if the plaintiff had standing, the December 2015 notice means that the plaintiff does not plausibly plead any claims predicated on Twitter's ratification of its employees' conduct (claims one through three and five through seven), and the statute of limitations bars all claims except the UCL claim (claim two).

The plaintiff does not meaningfully dispute that Twitter sent notices in December 2015. (Indeed, Twitter submitted its notification lists showing notice to the plaintiff.[58]) Instead (in his opposition brief), the plaintiff asserts that he may not have received the notice (because of "AI-based filtering software") and that Twitter could have done more, such as sending a text message to the phone number associated with his account.[59] But the December 2015 notice defeats any

[56] FAC – ECF No. 38 at 18 (¶ 93).

[57] *Id.* at 20–21 (¶¶ 107–109).

[58] Recipient Lists, Exs. 3 & 4 to Twitter Employee Decl. – ECF Nos. 40-10 & 40-11.

[59] Opp'n – ECF No. 58 at 19.

claim that Twitter ratified its employees' conduct, which disposes of claims one through three (the SCA, UCL, and invasion-of-privacy claims, all predicated on a ratification theory). Similarly, the claims of intentional and negligent misrepresentation and concealment (claims five, six, and seven) are grounded on the February 2016 notice about the bug, but any argument that the February notice increased confusion is defeated by the actual notice in December 2015.

Moreover, providing a job and access to its platform and user information does not establish Twitter's *respondeat superior* liability for its rogue employees' unauthorized spying for Saudi operatives. *Lisa M. v. Henry Mayo Newhall Mem'l Hosp.*, 12 Cal. 4th 291, 298 (1995). To the contrary, Alzabarah and Abouammo are — under the complaint's allegations — demonstrably not acting in the scope of their employment and instead were acting as agents for the Saudi regime.

The December 2015 notice also means that all claims but the UCL claim are barred by the statute of limitations. The SCA, invasion-of-privacy, and negligent-hiring claims each have two-year statutes of limitations.[60] The intentional-misrepresentation, negligent-misrepresentation, and concealment claims each have three-year statutes of limitations.[61] (The UCL claim has a four-year statute of limitations.[62])

1.3 Other Defects

The plaintiff does not plead his misrepresentation and concealment claims with particularity. Fed. R. Civ. P. 9(b). The February 2016 notice — standing alone or viewed in the context of the December 2015 notices — is not on its face false or misleading. As to the claims of negligent hiring, supervision, or retention of employees, the plaintiff's allegations — that there were "red flags" and known risks — are conclusions, not facts.[63] The UCL claim fails too: the predicate

---

[60] 18 U.S.C. § 2707(f) (SCA); Cal. Civ. Proc. Code § 335.1 (claims for injury to a person); *Quan v Smithkline Beecham Corp.*, 149 F. App'x 668, 670 (9th Cir. 2005) (invasion-of-privacy claim); *Kaldis v. Wells Fargo Bank, N.A.*, 263 F. Supp. 3d 856, 867 (C.D. Cal. 2017) (negligent-hiring claim).

[61] Cal. Civ. Code § 338(d) (fraud or mistake); *R. Power Biofuels, LLC v. Chemex, LLC*, No. 16-CV-00716-LHK, 2016 WL 6663002, at *12 (N.D. Cal. Nov. 11, 2016) (intentional-misrepresentation and concealment claims); *Fanucci v. Allstate Ins. Co.*, 638 F. Supp. 2d 1125, 1133 n.5 (N.D. Cal. 2009) (negligent-misrepresentation claim).

[62] *Aryeh v. Canon Bus. Sols. Inc.*, 55 Cal. 4th 1185, 1192 (2013) (citing Cal. Bus. & Prof. Code § 17208).

[63] FAC – ECF No. 38 at 13 (¶ 68).

violation is the SCA claim, there is no viable fraud claim, and the plaintiff did not identify an unfair business practice. Cal. Bus. & Prof. Code § 17200 (forbidding unlawful, unfair, and fraudulent business practices).

2. McKinsey's Motion to Dismiss

The plaintiff sued McKinsey for intentional infliction of emotional distress, a claim that he predicates on McKinsey's allegedly identifying him to Saudi authorities — based on internal Twitter data — as shaping opinion in Saudi Arabia.[64] McKinsey moved to dismiss for lack of personal jurisdiction and for failure to state a claim.[65]

"In opposing a defendant's motion to dismiss for lack of personal jurisdiction, the plaintiff bears the burden of establishing that jurisdiction is proper." *Ranza v. Nike, Inc.*, 793 F.3d 1059, 1068 (9th Cir. 2015) (quotation omitted). "The general rule is that personal jurisdiction is proper if permitted by a long-arm statute and if the exercise of that jurisdiction does not violate federal due process." *Pebble Beach v. Caddy*, 453 F.3d 1151, 1154–55 (9th Cir. 2005) (analyzing the California and federal long-arm statutes). "Because 'California's long-arm statute allows the exercise of personal jurisdiction to the full extent permissible under the U.S. Constitution,' [a court's] inquiry centers on whether exercising jurisdiction comports with due process." *Picot v. Weston*, 780 F.3d 1206, 1211 (9th Cir. 2015) (quoting *Daimler AG v. Bauman*, 571 U.S. 117, 125 (2014)). The due-process inquiry is whether the defendant has sufficient minimum contacts with the forum such that the assertion of jurisdiction in the forum "'does not offend traditional notions of fair play and substantial justice.'" *Pebble Beach*, 453 F.3d at 1154–55 (quoting *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 315 (1945)).

[64] FAC – ECF No. 38 at 25–26 (¶¶ 139–45).

[65] McKinsey Mot. – ECF No. 43.

"There are two types of personal jurisdiction: general and specific." *Bristol-Myers Squibb Co. v. Super. Ct.*, 137 S. Ct. 1773, 1779–80 (2017). In his opposition, the plaintiff asserts only general — and not specific — jurisdiction over McKinsey.[66]

"A court with general jurisdiction may hear *any* claim against that defendant, even if all the incidents underlying the claim took place in a different jurisdiction. *Id.* at 1780 (emphasis in original) (citing *Goodyear Dunlop Tire Ops., S.A. v. Brown*, 564 U.S. 915, 919 (2011)). "[A] plaintiff invoking general jurisdiction must meet an 'exacting' standard for the minimum contacts required." *Ranza*, 793 F.3d 1059 at 1069 (citation omitted). "A court may assert general jurisdiction over foreign (sister-state or foreign-country) corporations to hear any and all claims against them when their affiliations with the State are so 'continuous and systematic' as to render them essentially at home in the forum State, i.e., comparable to a domestic enterprise in that State." *Daimler*, 571 U.S. at 127 (quotation omitted). Such contacts must be "constant and pervasive." *Id.* at 122. "The paradigmatic locations where general jurisdiction is appropriate over a corporation are its place of incorporation and its principal place of business." *Ranza*, 793 F.3d at 1069 (citing *Daimler*, 571 U.S. at 133 n.11). "Only in an exceptional case will general jurisdiction be available anywhere else." *Id.* (quotation omitted).

The claim against McKinsey has no connection to the forum. McKinsey is incorporated in New York and has its headquarters there. There is no general personal jurisdiction.

CONCLUSION

The court grants the defendants' motions to dismiss. The plaintiff must file any amended complaint by August 27, 2020 and provide a blackline of the original complaint as an attachment. If he does not, the court will enter judgment in favor of the defendants.

IT IS SO ORDERED.

Dated: August 12, 2020

LAUREL BEELER
United States Magistrate Judge

[66] Opp'n – ECF No. 52 at 6–8.